

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
TARGET ACCOUNT, more fully described in
Attachment A

Case No. MJ20-614

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

TARGET ACCOUNT, more fully described in Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

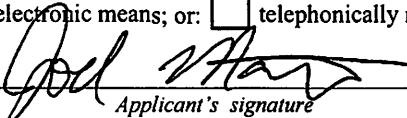
Code Section	Offense Description
18 U.S.C §§ 1343, 1030, 1029, 371, and 1349	Wire Fraud, Computer Fraud and Abuse, Access Device Fraud, and Conspiracy to Commit such Offenses

The application is based on these facts:

- ☒ See Affidavit of Special Agent Joel Martini, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Joel Martini, FBI Special Agent
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: September 24, 2020


Judge's signature

City and state: Seattle, Washington

Michelle L. Peterson, United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
 COUNTY OF KING)

I, Joel Martini, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed since January 2017. I am assigned to the Cyber squad where I primarily investigate computer intrusions and other Cybercrimes. My experience as an FBI Agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, Cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I have received advanced training in the acquisition and analysis of digital evidence (both network and host based), responding to computer intrusions and other incidents. I currently hold a Bachelor's of Science in Information Systems from Corban University.

2. Prior to my employment as a Special Agent, I worked as a Computer Forensic Examiner for the FBI for approximately 5 years. As part of that employment, I became familiar with the design and operations of various electronic devices, networks, and websites, including technology described herein.

3. I make this affidavit in support of an application for a search warrant for data and information associated with a certain account ("Target Account") stored at premises controlled by an electronic communications service and/or remote computer service provider ("Provider"), referenced below. The information to be searched is

described in the following paragraphs and in Attachment A, which is incorporated herein. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC (“Google”), located at 1600 Amphitheatre Parkway, Mountain View, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B, pertaining to the following account(s), identified in Attachment A:

- **deletescape@gmail.com**

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. This warrant is requested in connection with an ongoing investigation in this district by the Seattle Field Office of the Federal Bureau of Investigation (FBI).

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, FBI computer scientists and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1343 (Wire Fraud), Section 1030 (Computer Fraud and Abuse), Section 1029 (Access Device Fraud), and 371 and 1349 (conspiracy to commit such offenses). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes, as described in Attachment B.

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by devices, such as computers and servers, on the Internet.

1 An IP address is often a series of four numbers, each in the range 0-255, separated by
 2 periods (e.g., 104.250.138.210). Every device attached to the Internet must be assigned
 3 an IP address so that Internet traffic sent from and directed to that device may be directed
 4 properly from its source to its destination. Most Internet service providers control a
 5 range of IP addresses (also known as an IP Block).

6 b. **Internet:** The Internet is a global network of computers and other
 7 electronic devices that communicate with each other. Due to the structure of the Internet,
 8 connections between devices on the Internet often cross state and international borders,
 9 even when the devices communicating with each other are in the same state.

10 c. **Browser:** A “web browser” or “browser” is a software program that
 11 allows a user to access web pages, primarily on the internet. Popular browsers include
 12 Google’s Chrome browser and Microsoft’s Edge and Explorer browsers.

13 d. **Source Code:** Source code is the list of human-readable
 14 instructions that a programmer writes when developing a program. When completed, a
 15 computer can understand and execute these coded instructions as provided by the
 16 developer.

17 **SUMMARY OF PROBABLE CAUSE**

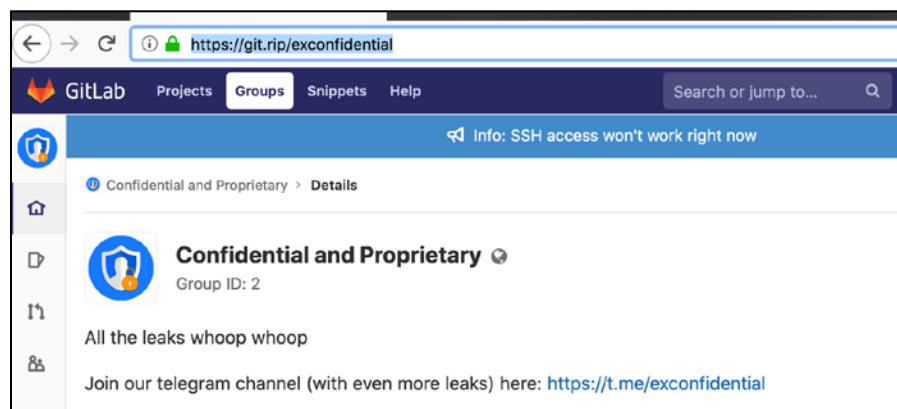
18 A. **Background**

19 7. The FBI is conducting an investigation into the hacking of various entities’
 20 computer databases and the subsequent theft and dissemination of information from those
 21 entities, including source code, confidential information, and internal user data. As
 22 discussed below, the targets of the investigation include a Swiss national named Till
 23 Kottmann, currently residing in Lucerne, Switzerland. Kottmann uses the alias
 24 “deletescape” across various online, email, and social media accounts, including Twitter,
 25 Instagram, and Facebook. As discussed below, Kottmann is believed to be the user of
 26 Google account associated with **deletescape@gmail.com** (Target Account). There is
 27 probable cause to conclude that the Target Account contains evidence of the user’s
 28 involvement in the criminal activity under investigation.

8. Kottmann, who has presented himself as a security researcher, predominantly has targeted “git” repositories belonging to companies in various countries, including the United States, among others. “Git” is a distributed version-control system for tracking changes in source code during software development in containers called repositories. It is designed for coordinating work among programmers, but it can be used to track changes in any set of files. GitLab, Gitea, and GitHub are examples of systems that use “git” repositories.

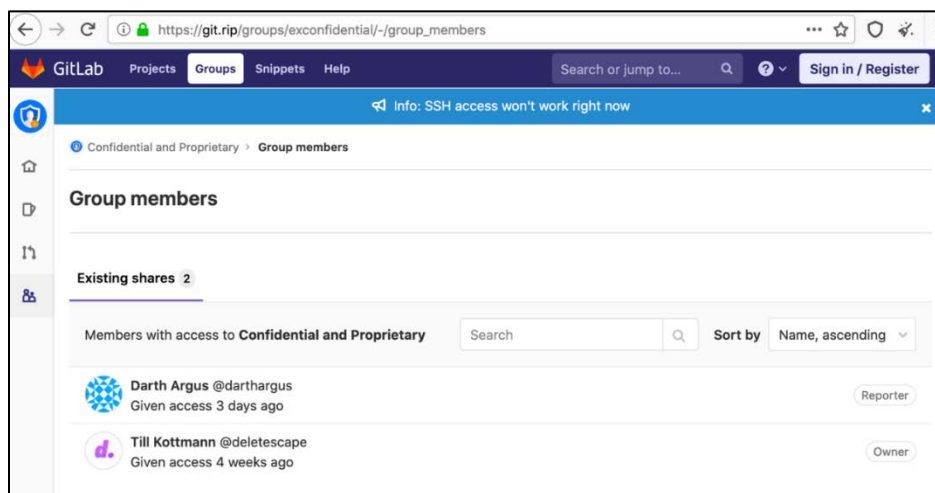
9. More specifically, Kottmann identified and accessed vulnerable “git” repositories through use of either stolen credentials and/or exploits allowing expansive permissions to new users. He then copied/cloned their contents to server(s) he controlled and thereafter publicly posted copies of the stolen data to his publicly available, data leaks website <http://git.rip> (“git.rip website”) and/or to his associated Telegram channel “ExConfidential.” He also distributed data through Mega, a cloud-based file storage and sharing service provider based in New Zealand. Kottmann also solicited and subsequently posted copies of additional data leaks from others in an effort to grow the popularity of his website/channel.

10. Kottmann’s git.rip website features a webpage (git.rip/exconfidential) that advertises “Confidential and Proprietary” data leaks. A screenshot is below:



The git.rip website also invites visitors to join “our” Telegram¹ channel for “even more leaks” and provides a link. As of August 2020, data dumps from more than 50 entities, including notable companies such as Microsoft, Google, Motorola, Qualcomm, Nestle, and Intel, are or were available for download on the git.rip website.

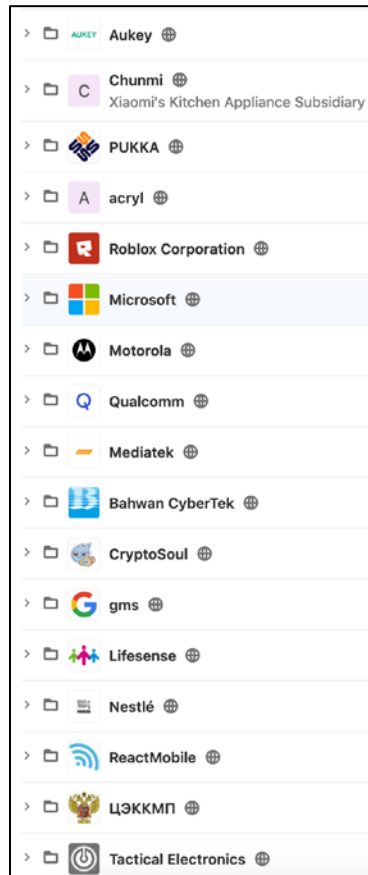
11. The “Users” tab on the git.rip/exconfidential page shows that one member of the site has “Owner” (read/write full admin permissions) access to the global Confidential and Proprietary group. This user has the name Till Kottmann and username @deletescape.



In addition to Kottmann, user @darthargus is listed as having Reporter (read permissions) access to Confidential and Proprietary. Under the Microsoft subgroup, user @myst33d has Maintainer (read/write partial admin permissions) access. Similarly, user @q3w3e3 is a Maintainer for the NNG group, @sdfasbhdhfsdfsdf and @PythonLimited are Maintainers for Qualcomm, @mtkdocs and Sean Hoyt (@Deadman96385) are Maintainers for Mediatek, @fevikul and @kotakat are Reporters for React Mobile, and @0xWHYME, @449274832, @Deepquest, @ligich, Evan (@cat), @Hexawolf, @xloem, @dat0rr1p0r, @fr3dd13, @kotakat, @rekt321, and Sydney Bizkut (@syd) are Reporters for Tactical Electronics.

¹ Telegram is a messaging service that provides for end-to-end encryption.
Affidavit of Special Agent Joel Martini
USAO# 2020R00400 - 5

12. The published downloadable databases include numerous U.S. companies as well as other foreign entities, including companies located in Switzerland, Germany, Taiwan, India, China, Ukraine, and Russia, among other countries. A sample excerpt from the git.rip website is below, which identifies the victim company by name and logo:




13. During the course of the investigation, additional entities and apparently hacked data have been added to (and removed from) the git.rip website. For instance, on about August 6, 2020, Kottmann published a trove of confidential technical material, code, and documents related to various processors and chipsets of U.S. chip manufacturer Intel. Kottmann later wrote on Twitter about the Intel data: “They were given to me by an anonymous source who breached them earlier this year, more details about this will be published soon.”² More recently, on about August 15, 2020, additional databases were

² See, e.g., <https://www.bleepingcomputer.com/news/security/intel-leak-20gb-of-source-code-internal-docs-from-alleged-breach/> (last visited 08/19/2020).

published on the git.rip website, including internal files and records related to the Washington State Department of Transportation (WSDOT).³

14. According to records from Namecheap, the U.S-based registrar for the git.rip domain, the domain is registered to an account in the name of Till Kottmann and username deletescape, created in March 2018, as shown in the excerpt below:

							
User Info							
Username User ID Account Locked	First Name Last Name Email	Support Pin Pin Expiry	Signup Date Signup IP	Account Balance Available Balance Earned Amount	Organization Street Address City, State	Phone Fax Country, Zip	Latest Transaction Latest Login Login IP
deletescape 4169892 No	Till Kottmann deletescape@gmail.com	Reset	3/30/2018 10:25:57 AM 92.105.162.17	0.0000 0.0000 0.0000	NA Brambergstrasse 25 Luzern, Luzern	+41-795259752 NA CH, 6004	7/31/2020 2:57:33 AM 7/28/2020 5:35:29 PM 81.6.38.253

The account subscriber information further included registered email address **deletescape@gmail.com**, phone number +41-79-525-9752, and an address in Luzern (Lucerne), Switzerland. According to public records, country code +41 refers to Switzerland, and the service provider for this phone number is Swisscom Mobile.

15. According to Namecheap account records, the git.rip domain was registered on or about November 18, 2019, and paid for with a credit card in the name “Till Kottmann.”

50387699 deletescape 11/18/2019 3:00:52 PM	a4818367-e1d4-4ce4-be0e-c0987ad982a5 ch_1fgGP0I2aKwfvOvmMQkeBzGh	\$17.06/ \$17.06 CREDIT CARD N/A	Type: register Domain Registration git.rip	Years : 1 Qty: 1 Price: 16.88	Successful: YES 200:Command completed successfully
			Type: purchase Free WhoisGuard	Years : 1 Qty: 1 Price: 0	Successful: YES Command completed successfully

57581260	deletescape 85.L65.224 (US)	a4818367-e1d4-4ce4-be0e-c0987ad982a5 ch_1fgGP0I2aKwfvOvmMQkeBzGh	PURCHASE CREDITCARD	\$17.06	APPROVED 90 / 10	...8346(01/2024) US / CH	11/18/2019 3:00:51 PM	50387699	Till Kottmann N/A	\$0.00 \$0.00
----------	--------------------------------	---------------------------------------------------------------------	------------------------	---------	---------------------	-----------------------------	--------------------------	----------	----------------------	------------------

In addition to git.rip, the account registered numerous domains, including tillie.dev, deletescape.cloud, letescape.de, and deletespace.ch.

16. As part of its investigation, the FBI downloaded and examined samples of the featured data leaks. All of the repositories analyzed appeared to contain source code as advertised. Some of the leaked code further contained passwords, credentials and

³ As further examples, on multiple dates, including on about May 4, 2020, Kottmann posted source code and other data of Microsoft. On about June 11, 2020, Kottmann posted a database purporting to belong to a video game developer headquartered within the Western District of Washington.

1 other items that enabled access to additional company networks or servers. The FBI also
2 interviewed numerous victim companies, which confirmed the authenticity of their data
3 that Kottmann published as well as the initial data breach and theft. None of the victims
4 had any association with Kottmann or “deletescape.”

5 17. For example, on April 28, 2020, I met with representatives from a company
6 called React Mobile, referred to herein as “Company A,” a provider of enterprise class
7 safety solutions (such as panic buttons) located in Seattle, Washington. Company A
8 reported that, in April 2020, a former employee discovered what he recognized to be the
9 company’s proprietary source code published on the git.rip website. According to
10 Company A, the stolen code available on the git.rip website was a mirror of the
11 company’s GitLab repository. GitLab is a platform that companies can install on their
12 infrastructure to store their codebase and change it with version control in digital
13 containers called repositories. Company A confirmed that the files on the git.rip website
14 were authentic, relatively recent, private, and electronically stored, indicating that an
15 unauthorized computer intrusion had taken place. After conducting an internal
16 investigation, Company A concluded that a hacker used an exploit in GitLab to gain
17 access to the company’s data and clone it to the git.rip website. As evident from activity
18 logs, the hacker created a new user account called “deletescape” to siphon the data on
19 their network.

20 18. Investigators determined that Company A’s data was posted to the git.rip
21 website on or about February 14, 2020. Similarly, records obtained from DigitalOcean,
22 discussed below, the hosting service for the git.rip site, show that, on the same date, user
23 “deletescape” (Kottmann) cloned Company A’s data to the of the git.rip website.

24 19. Additionally, I have spoken with special agents from FBI Oklahoma City
25 who interviewed representatives of another company called Tactical Electronics, referred
26 to herein as “Company B,” based in Broken Arrow, Oklahoma. Company B contacted
27 their office to report and confirm that they suffered a data breach similar to that described
28 by Company A. As seen in the screenshot above, one of the repositories available on the

git.rip website features Company B's name and logo.⁴ Company B's data was posted on or about April 15, 2020. Similarly, records obtained from DigitalOcean show that, on about the same date, user "deletescape" (Kottmann) cloned Company B's data to the git.rip website. Further, Company B conveyed to FBI that the credentials (username and password) of one of its employees, a senior design engineer with initials R.D., were used as part of the commission of the intrusion.

20. Kottmann has openly disclosed and discussed his conduct on various online platforms, including Twitter, and with media outlets. For instance, on about May 17, 2020, Kottmann "tweeted" from his Twitter account @deletescape reference to his dissemination of companies' private source code:

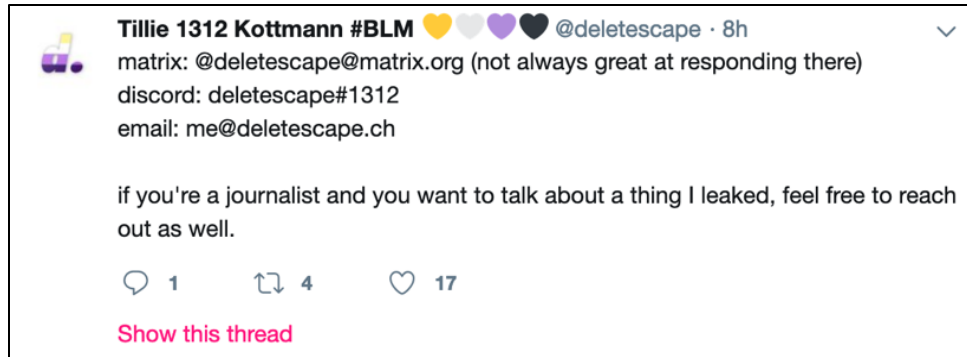


In other "tweets," Kottmann has solicited hacked data to leak, expressly inviting others with "access to any confidential info, documents, binaries or source code, which you think should be made available to the public," to contact him:



He also posted his contact information, which incorporated the moniker "deletescape," and invited media inquiries about his data leaks:

⁴ Other companies, including Intel, Microsoft, and Qualcomm, similarly have confirmed the legitimacy of data posted by Kottmann and an associated hack of their data. Others, such as Nestle, confirmed that the published data did indeed come from their servers but were unaware of a prior hack or how the data was stolen.



As reported by media outlets, Kottmann has acknowledged his and his associates' conduct in interviews, although he claimed to take steps to mitigate the damage to the victim companies from his data leaks.⁵ Through these and other messages and through published interviews, Kottmann confirmed his use of the online alias "deletescape."

21. The git.rip website was hosted by DigitalOcean, a U.S. service provider, at a particular IP address. According to records and information provided by DigitalOcean, the IP address was associated with a Digital Ocean account created on August 30, 2019, using IP address 195.245.237.179, and registered to the customer email, me@deletescape.ch,⁶ name "Till Kottmann", User ID 6507364, and location of Lucerne, Switzerland. The specific "droplet" associated with the IP address hosting the git.rip website was created on December 20, 2019, under the name "Deletescape-cloud."

22. Further, account logs of this user's login activity show IP addresses that resolve to SwissCom, a major Internet service provider in Switzerland. The chart below includes descriptions of some of the IP addresses used to access Kottmann's DigitalOcean account and specifically the git.rip database:

IP	Date(s)	Provider	Relevance
195.245.237.179	2019-08-30 13:46:06 UTC	Fenaco Genossenschaft	Account creation Account login activity

⁵ See, e.g., <https://tech.hindustantimes.com/tech/news/swiss-developer-get-access-to-microsoft-nintendo-and-other-big-firm-s-source-codes-revealing-confidential-information-71595925484091.html> (last visited 08/09/2020); <https://www.bleepingcomputer.com/news/security/source-code-from-dozens-of-companies-leaked-online/> (last visited 08/09/2020).

⁶ According to public records, Google is the domain registrar deletescape.ch, but the domain is hosted by hostserv.eu.

IP	Date(s)	Provider	Relevance
178.197.235.208	2020-01-08 20:06:12 UTC	Swisscom AG	Account login activity
83.79.177.129	2020-01-09 20:06:01 UTC	Swisscom AG	Account login activity
85.1.85.224	2020-03-10 09:40:26 UTC	Swisscom AG	Account login activity Admin login for git.rip database
92.104.30.47	2020-04-28 03:37:00 UTC	Bluewin; Swisscom AG	Admin login for git.rip database

Further, four of the five above-listed IP addresses also were used to access the domain registrar account at Namecheap used to register the git.rip domain.

23. According to records from Twitter, Twitter account @deletescape (account ID 3089774218) was registered in March 2015, and is associated with email me@deletescape.ch and phone number +41-79-525-9752. This is the same Swiss phone number associated with the Namecheap account used to register the git.rip domain. Furthermore, according to account login logs, IP address 92.104.30.47 was used to log into Twitter account @deletescape on numerous (more than 90) occasions between April 1, 2020 and May 1, 2020. These account logins include multiple logins using this same IP address on April 28, 2020, which is the same date the IP address was used for admin access of the git.rip database.

24. On about August 10, 2020, I discovered that account @deletescape had been suspended by Twitter, apparently for violations of the platform's terms of service. Although the basis for this account action is unknown to me, this suspension appears to have occurred shortly after Kottmann tweeted about his data leak from the well-publicized hack of Intel.⁷

25. Through further investigation, investigators identified another, recently-created Twitter account that appears to be used by Kottmann, specifically, Twitter

⁷ Based on my training and experience and that of other experienced investigators, and my review of Twitter terms of service, I know that Twitter account suspensions can be temporary or permanent, Twitter may remain in possession of data and content related to suspended accounts, and Twitter users may in some cases be able to reinstate or unsuspend suspended accounts. See, e.g., <https://help.twitter.com/en/managing-your-account/suspended-twitter-accounts>

1 username @antiproprietary. As set forth in the screenshot below, Twitter account
 2 @antiproprietary was created in August 2020, notably approximately when @deletescape
 3 was suspended, and associated with Kottmann's known moniker "deletescape" (albeit
 4 stating "definitely not deletescape"):



16 The account also uses the screenname "Confidential & Proprietary," which is a phrase
 17 that likewise appeared on the git.rip website, and acknowledged the user's hacking
 18 activity and "Antiproprietary Action." The user (Kottmann) refers to himself as a
 19 "hacktivist," which is a term that commonly refers to a person who gains unauthorized
 20 access to computer files or networks in order to further social or political ends.⁸

21 26. Activity from Twitter account @antiproprietary also indicates that the
 22 account user is the same user of @deletescape (Kottmann). For instance, on August 10,
 23 2020, Twitter account @antiproprietary sent a series of tweets referencing "deletescape,"
 24 including substantively identical messages previously posted by @deletescape. Those
 25 included, among others, (i) a tweet identifying his contact information, which
 26
 27
 28

⁸ See, e.g., <https://en.wikipedia.org/wiki/Hacktivism> (last visited 08/19/2020)

incorporated the “deletescape” moniker and invited media inquiries, and (ii) a tweet soliciting source code:





He also posted (likely sarcastically) about “not” being @deletescape, and @antiproprietary “not” being used to evade a “ban,” which is apparent reference to the account suspension of @deletescape:



On August 12, 2020, Twitter account @antiproprietary (Kottmann) posted (possibly jokingly) about arguing that his and his associates’ (“me hacking corps”) hacking activity and publication of stolen data amounted to a form of free speech:



Based on my training and experience, I am familiar with this ideology, which is not uncommon among certain hacktivists.

27. Investigators have requested subscriber records for Twitter account @antiproprietary, but to date responsive data has not yet been received and reviewed. However, there is ample probable cause to conclude that the user of both Target Accounts are the same person and that that person is Kottmann.

28. On about September 15, 2020, a judge in this federal district issued an arrest warrant for Kottmann, under seal, based on a criminal complaint charging him with one count of conspiracy to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030). At this time and at all times material to this investigation, Kottmann is believed to be located in Switzerland and otherwise a foreign country.

B. Summary of Target Account

29. There is probable cause to believe that the user of the Google account associated with **deletescape@gmail.com** is involved in criminal activity, including the Target Offenses discussed herein, and that the data and information relating to the Target Account, including content, include evidence of criminal activity, attribution, and the location of the account user(s).

30. According to records obtained from Google, the account associated with **deletescape@gmail.com** (Target Account) is registered in the name "Till Kottmann," as shown in the excerpt below:

GOOGLE SUBSCRIBER INFORMATION

Google Account ID: 660542396895
 Name: Till Kottmann
 e-Mail: deletescape@gmail.com
 Alternate e-Mails: deletescape@outlook.com

Created on: 2013-05-31 07:18:48 UTC
 Terms of Service IP: 62.202.56.42

Services: Web & App Activity, Gmail, Google Photos, Google Hangouts, Google Chrome Sync, Chrome Web Store, Google Developers Console, Google Play Console, Blogger, Google Drive, Google Docs, Fusion Tables (experimental), Google Voice, Google Cloud Print, Android, Google Calendar, Location History, Google Maps Engine, Google Play, Google My Business, Google Analytics, Android Device Console, Tasks in Tingle, Google URL Shortener, Google AdSense, Youtube Analytics Storage, Google Developers Console, Google My Maps, Google Search Console, Chromeos Login, Google Payments, Google Translator Toolkit, Google Sites, Google Developers Console, Has Madison Account, Google Play Music, YouTube, Gerrit Code Review, Google Play artist hub, Google Takeout, Buganizer, Google Groups, Google AdWords, Google Keep, Api.ai Developer, Material Gallery, Android Partner, Google Domains, Is In Family, Onetoday, Google Developers Console

Deletion Date:
 Deletion IP:

Last Logins: 2020-06-19 15:06:17 UTC, 2020-06-19 14:02:20 UTC, 2020-06-19 12:56:29 UTC

ACCOUNT RECOVERY

Recovery e-Mail: me@deletescape.ch
 Recovery SMS: +41795259752 [CH]

PHONE NUMBERS

Signin Phone Numbers: +41787130708, +41795259752, +41795259752 [CH]
 2-Step Verification Phone Numbers: +41795259752 [CH]

The account was created in May 2013 and remained active as of the production date.⁹

The recovery email is me@deletescape.ch, which is same email associated with the @deletescape Twitter account and the DigitalOcean account used to host the git.rip site. Further, the associated phone numbers include +41-79-525-9752, which is same Swiss phone number associated with the @deletescape Twitter account and the Namecheap account used to register the git.rip domain.

31. According to Google records, the Target Account is further associated with alternate email deletescape@outlook.com. According to records from Microsoft, the provider of outlook.com accounts, this associated deletescape email account also is registered in the name “Till Kottmann” of Switzerland, as shown below:

Query for: deletescape@outlook.com									
Date Range: 1/1/2018 12:00:00 AM to 5/5/2020 11:59:59 PM									
Record Type (Registration)	Signin Name	First Name	Last Name	State	Postal Code	Country	Time Zone	PUID	Alternate Email
Registration Profile	deletescape@outlook.com	Till	Kottmann		8000	Switzerland	Zurich, Switzerland - CET	00037FFEB7E1F369	deletescape;till_kottmann@outlook.com


This outlook account is also associated with alias names “deletescape” and till_kottmann@outlook.com.

⁹ The Google account records for the Target Account were produced on or about June 19, 2020.

32. According to IP activity logs produced by Google, the account associated with **deletescape@gmail.com** (Target Account) was accessed using IP addresses encountered elsewhere in the investigation. For instance, on numerous occasions between September 18, 2019 and May 5, 2020 (the date range of IP activity produced), multiple IP addresses used to access the DigitalOcean account associated with the git.rip site (including, 83.79.177.129, 85.1.85.224, and 92.104.30.47) also were used to login to the Target Account. In fact, IP address 92.104.30.47 accessed both accounts on April 28, 2020.

33. As set forth above, **deletescape@gmail.com** is the email address associated with the Namecheap account used to register the git.rip domain. Accordingly, there is probable cause to conclude that the Target Account will contain emails and other information related to the Namecheap account used to register the git.rip domain and others.

34. Further, according to transaction activity for the Namecheap account,¹⁰ the user (Kottmann) made numerous purchases using one or more credit cards in the name “Till Kottmann” as well as using an account at Paypal, an online payment service. That Paypal account appears to be registered to email **deletescape@gmail.com**, and was used on multiple occasions between March 2018 and as recently as September 10, 2020, to make payments in the Namecheap account, as shown in the excerpts below:

											
Transaction Review											
ID	Username IP (Country)	CC Order ID CC Transaction ID	Transaction Type Payment Source	Amount	Status Score	CC-L4(exp) Country IP / Bill	Date (PST)	Order ID	Name on Card Email	Balance Before	Balance After
71017582	deletescape 178.197.226.253 (N/A)	178.197.226.253-DELETESCAPE-IOS-TRAN:71017582- 1599148160.390 6M7219877K9392419	PURCHASE PAYPAL	\$29.96	COMPLETED 0 / 0	...(N/A) N/A / N/A	9/10/2020 2:55:52 PM	62131518	N/A deletescape@gmail.com	\$0.00	\$0.00
71017537	deletescape 178.197.226.253 (N/A)	178.197.226.253-DELETESCAPE-IOS-TRAN:71017537- 1599749660.20 6D581121FG829715G	PURCHASE PAYPAL	\$14.98	COMPLETED 0 / 0	...(N/A) N/A / N/A	9/10/2020 2:54:13 PM	62131480	N/A deletescape@gmail.com	\$0.00	\$0.00
70339179	deletescape 127.0.0.1 (N/A)	27996cd9-bf83-4ac4-aa76-e46d7164f01 zh_1HM61x2aKwfrOumio5aYVc	PURCHASE CREDITCARD	\$23.06	APPROVED 0 / 0	...8346(N/A) N/A / N/A	8/31/2020 1:58:10 AM	61534918	Till Kottmann N/A	\$0.00	\$0.00

39565810	deletescape 92.105.162.17 (N/A)	92.105.162.17-DELETESCAPE-NC-TRAN:39565810- 1522406014.927 4VH85523LM296615T	PURCHASE PAYPAL	\$3.88	COMPLETED 0 / 0	...(N/A) N/A / N/A	3/30/2018 10:33:31 AM	33910386	N/A deletescape@gmail.com	\$0.00	\$0.00

¹⁰ The Namecheap account records were produced on or about September 11, 2020.

1 35. Additionally, a Paypal account associated with **deletescape@gmail.com**
2 (Target Account) also was used for payments for the DigitalOcean account used to host
3 the git.rip site. As discussed above, the account is registered in the name “Till
4 Kottmann” of Lucerne, Switzerland. According to transaction records provided by
5 DigitalOcean related to the account, the account holder made a payment using a Paypal
6 account associated with email **deletescape@gmail.com** (Target Account) on August 30,
7 2019, which is the same date the account was created. This Paypal account also was used
8 to make payments on the DigitalOcean account on multiple subsequent dates in January,
9 February, March, and April 2020.

10 36. Investigators have requested records for the Paypal account associated with
11 **deletescape@gmail.com** (Target Account), but to date responsive data has not yet been
12 received and reviewed. Based on my training and experience, I know that Paypal account
13 holders typically receive account notifications, sent to the designated associated email
14 account, of certain account activity, including when payments are sent or received and
15 when accounts settings are made. Accordingly, I believe there is ample probable cause to
16 believe that **deletescape@gmail.com** (Target Account) will contain emails relating to a
17 Paypal account used to facilitate the scheme under investigation.

18 37. According to Google account records, the account associated with
19 **deletescape@gmail.com** (Target Account) remained actively accessed from
20 September 18, 2019, through May 5, 2020 (the date range of IP activity produced).
21 Moreover, the records reflect a last login of June 19, 2020 (on about the date of Google’s
22 production). Moreover, I know that users of online accounts such as Google may, in fact
23 often, remain logged into accounts for extended periods of time. I also note that this time
24 period of account usage corresponds with the criminal activity under investigation.

25 38. Based on my training and experience, I know that Google logs and retains a
26 substantial amount of information about its customers. For instance, unless specific steps
27 are taken to change default settings or to conceal or delete records of activity, this
28 information should include, among many other things, customers’ Internet activity,

1 including their web browsing and search history, while logged into a Google account or
2 through a Google product, such as Chrome. I also know that the type of crime at issue
3 here necessitates use of the Internet and electronic devices. As discussed herein,
4 Kottmann was very active on various online accounts and is suspected of using the
5 Internet to clone and publish stolen victim data. I also know that individuals involved in
6 cybercrime and other fraud often use the Internet to research and facilitate their activities
7 and that evidence of such conduct often appear in browsing and search history and other
8 data stored by Google. I also know that, unless specific steps are taken to change default
9 settings or to conceal or delete records of activity, Google captures location data related
10 to some of its services. Based on my training and experience, such information often
11 serves as evidence of attribution, that is, of the user or users of the account, and assists in
12 locating the subjects of investigation and additional evidence. Accordingly, there is
13 probable cause to believe that Google possesses information that is evidence of criminal
14 conduct and evidence establishing those participating therein.

15 39. The Target Account was the subject of a prior preservation request served
16 upon Provider, as set forth below:

17 a. Google account associated with **deletescape@gmail.com**: Google
18 reference #3924850 (August 10, 2020).

19 **BACKGROUND OF GOOGLE SERVICES**

20 40. In my training and experience, I have learned that Google provides a wide
21 variety of on-line services, including electronic mail (“e-mail”) access and instant
22 messaging (otherwise known as “chat” messaging), to the general public. Google
23 provides subscribers e-mail and chat accounts at the domain name “@gmail.com.”
24 Google also allows subscribers to register a custom domain name and set up Google
25 services such as chat and e-mail using that domain name instead of “@gmail.com.”
26 Google also hosts domains and provides a multitude of services that can be linked and
27 managed through a common account.
28

1 **A. Subscriber Records and Account Content**

2 41. Subscribers obtain an account by registering with Google. When doing so,
3 e-mail providers like Google ask the subscriber to provide certain personal identifying
4 information. This information can include the subscriber's full name, physical address,
5 telephone numbers and other identifiers, alternative e-mail addresses, and, for paying
6 subscribers, means and source of payment (including any credit or bank account number).
7 In my training and experience, such information may constitute evidence of the crimes
8 under investigation because the information can be used to identify the account's user or
9 users, and to help establish who has dominion and control over the account.

10 42. E-mail providers typically retain certain transactional information about the
11 creation and use of each account on their systems. This information can include the date
12 on which the account was created, the length of service, records of log-in (i.e., session)
13 times and durations, the types of service utilized, the status of the account (including
14 whether the account is inactive or closed), the methods used to connect to the account
15 (such as logging into the account via Google's websites), and other log files that reflect
16 usage of the account. In addition, e-mail providers often have records of the Internet
17 Protocol address ("IP address") used to register the account and the IP addresses
18 associated with particular logins to the account. Because every device that connects to
19 the Internet must use an IP address, IP address information can help to identify which
20 computers or other devices were used to access the e-mail account.

21 43. In some cases, e-mail account users will communicate directly with an e-
22 mail service provider about issues relating to the account, such as technical problems,
23 billing inquiries, or complaints from other users. E-mail providers typically retain
24 records about such communications, including records of contacts between the user and
25 the provider's support services, as well records of any actions taken by the provider or
26 user as a result of the communications. In my training and experience, such information
27 may constitute evidence of the crimes under investigation, because the information can
28 be used to identify the account's user or users.

1 44. In general, an e-mail that is sent to a Google subscriber is stored in the
2 subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail.
3 When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via
4 the Internet to Google servers, and then transmitted to its end destination. Google often
5 maintains a copy of received and sent e-mails. Unless the sender specifically deletes an
6 e-mail from the Google server, the e-mail can remain on the system indefinitely. Even if
7 the subscriber deletes the e-mail, it may continue to be available on Google's servers for
8 some period of time.

9 45. A sent or received e-mail typically includes the content of the message,
10 source and destination addresses, the date and time at which the e-mail was sent, and the
11 size and length of the e-mail. If an e-mail user writes a draft message but does not send
12 it, that message may also be saved by Google but may not include all of these categories
13 of data.

14 46. In addition to e-mail and chat, Google offers subscribers numerous other
15 services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome
16 Sync, Google Cloud Print, G-Suite, Google Developers Console, Google Drive, Google
17 Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console,
18 Google Voice, Google+, Google Profile, Location History, Web & Activity, and
19 YouTube, among others. Among other things, Google Search Console records a Google
20 account user's search queries. Google Web & Activity records certain browsing history
21 depending on whether the account holder is logged into their account. Like many
22 internet service companies, the services Google offers are constantly changing and
23 evolving.

24 47. Search and browsing history can also be extremely useful in identifying
25 those using anonymous online accounts and may also constitute direct evidence of the
26 crimes under investigation to the extent the browsing history or search history might
27 include searches and browsing history related to computer intrusions, victims, trafficking
28

1 in stolen data and other evidence of the crimes under investigation or indications of the
2 true identity of the account users.

3 48. Google is also able to provide information that will assist law enforcement
4 in identifying other accounts associated with the TARGET ACCOUNT, namely,
5 information identifying and relating to other accounts used by the same subscriber. This
6 information includes any forwarding or fetching accounts¹¹ relating to the TARGET
7 ACCOUNT, all other Google accounts linked to the TARGET ACCOUNT because they
8 were accessed from the same computer (referred to as “cookie overlap”), all other Google
9 accounts that list the same SMS phone number as the TARGET ACCOUNT, all other
10 Google accounts that list the same recovery e-mail address¹² as do the TARGET
11 ACCOUNT, and all other Google accounts that share the same creation IP address as the
12 TARGET ACCOUNT. Information associated with these associated accounts will assist
13 law enforcement in determining who controls the TARGET ACCOUNT and will also
14 help to identify other e-mail accounts and individuals relevant to the investigation.

15 **B. Google Location History and Location Reporting**

16 49. According to Google’s website, “Location Reporting” allows Google to
17 periodically store and use a device’s most recent location data in connection with the
18 Google Account connected to the device. “Location History” allows Google to store a
19 history of location data from all devices where a user is logged into their Google Account
20 and has enabled Location Reporting. According to Google “when you turn on Location
21 Reporting for a device like your iPhone or iPad, it lets Google periodically store and use
22 that device’s most recent location data in connection with your Google Account.” How
23 often Location Reporting updates location data is not fixed. Frequency is determined by
24

25 ¹¹ A forwarding or fetching account related to the TARGET ACCOUNT would be a separate e-mail account that can
26 be setup by the user to receive copies of all of the e-mail sent to the TARGET ACCOUNT.

27 ¹² The recovery e-mail address is an additional e-mail address supplied by the user that is used by Google to confirm
28 your username after you create an e-mail account, help you if you are having trouble signing into your Google
account or have forgotten your password, or alert you to any unusual activity involving user’s Google e-mail
address.

1 factors such as how much battery life the device has, if the device is moving, or how fast
2 the device is moving. Google's location services may use GPS, Wi-Fi hotspots, and
3 cellular network towers to determine an account holder's location.

4 50. Based on the above, I know that if a user of the TARGET ACCOUNT
5 utilizes a mobile device to access the respective account identified in Attachment A and
6 has not disabled location services on his or her device/s or through the Google account
7 settings, Google may have detailed records of the locations at which the account holders
8 utilized the mobile device/s. This type of evidence may further assist in identifying the
9 account holders, and lead to the discovery of other evidence of the crimes under
10 investigation.

11 51. I know that Google's Android service collects and stores identifying
12 information about an Android smart phone used to access the Google account, including
13 the International Mobile Equipment Identifier (IMEI), International Mobile Subscriber
14 Identity (IMSI), telephone number and mobile carrier code. I know that Google's
15 Location History service periodically queries the physical location of a device that is
16 currently accessing a Google account through the device's GPS, nearby Wi-Fi network
17 IDs and cellular tower information and records a history of device movements in
18 Google's servers.

19 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

20 52. I anticipate executing this warrant under the Electronic Communications
21 Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by
22 using the warrant to require Provider to disclose to the government copies of the records
23 and other information (including the content of communications) particularly described in
24 Section I of Attachment B. Upon receipt of the information described in Section I of
25 Attachment B, government-authorized persons will review that information to locate the
26 items described in Section II of Attachment B.

27 53. Pursuant to Title 18, United States Code, Section 2703(g), this application
28 and affidavit for a search warrant seeks authorization to permit Provider, and its agents

1 and employees, to assist agents in the execution of this warrant. Once issued, the search
2 warrant will be presented to Provider with direction that it identify the account described
3 in Attachment A to this affidavit, as well as other subscriber and log records associated
4 with the accounts, as set forth in Section I of Attachment B to this affidavit.

5 54. The search warrant will direct Provider to create an exact copy of the
6 specified server, account and records.

7 55. I, and/or other law enforcement personnel will thereafter review the copy of
8 the electronically stored data, and identify from among that content those items that come
9 within the items identified in Section II to Attachment B, for seizure.

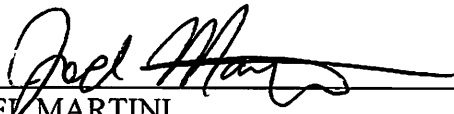
10 56. Analyzing the data contained in the copy of the specified account may
11 require special technical skills, equipment, and software. It could also be very time-
12 consuming. Searching by keywords, for example, can yield thousands of “hits,” each of
13 which must then be reviewed in context by the examiner to determine whether the data is
14 within the scope of the warrant. Merely finding a relevant “hit” does not end the review
15 process. Keywords used originally need to be modified continuously, based on interim
16 results. Certain file formats, moreover, do not lend themselves to keyword searches, as
17 keywords, search text, and many common e-mail, database and spreadsheet applications
18 do not store data as searchable text. The data may be saved, instead, in proprietary non-
19 text format. And, as the volume of storage allotted by service providers increases, the
20 time it takes to properly analyze recovered data increases, as well. Consistent with the
21 foregoing, searching the recovered data for the information subject to seizure pursuant to
22 this warrant may require a range of data analysis techniques and may take weeks or even
23 months. All forensic analysis of the data will employ only those search protocols and
24 methodologies reasonably designed to identify and seize the items identified in Section II
25 of Attachment B to the warrant.

26 CONCLUSION

27 57. Based on the forgoing, I request that the Court issue the proposed search
28 warrant. This Court has jurisdiction to issue the requested warrant because it is “a court

1 of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a),
 2 (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . .
 3 that - has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).
 4 Pursuant to 18 U.S.C. § 2703(g), the government will execute this warrant by serving the
 5 warrant on the Provider. Because the warrant will be served on the Provider, who will
 6 then compile the requested records and data, reasonable cause exists to permit the
 7 execution of the requested warrant at any time in the day or night. Accordingly, by this
 8 Affidavit and Warrant, I seek authority for the government to search all of the items
 9 specified in Section I, Attachment B (attached hereto and incorporated by reference
 10 herein) to the Warrant, and specifically to seize all of the data, documents and records
 11 that are identified in Section II to that same Attachment.

12 58. The affidavit and application are being presented by reliable electronic
 13 means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).
 14

15
 16 
 17 JOEL MARTINI
 18 Special Agent
 19 Federal Bureau of Investigation

20 The above-named agent provided a sworn statement attesting to the truth of the
 21 foregoing affidavit on 24th day of September, 2020.
 22

23
 24 
 25 MICHELLE L. PETERSON
 26 United States Magistrate Judge
 27
 28

ATTACHMENT A
Property to Be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data (including, but not limited to, Google Reference No. 3924850) associated with the following account(s):

- **deletescape@gmail.com**

(collectively, "TARGET ACCOUNT"), as well as all other subscriber and log records associated with each account, which are located at premises owned, maintained, controlled or operated by Google LLC, an electronic communications and online service provider headquartered at 600 Amphitheatre Parkway, Mountain View, California.

Google Reference #3924850

ATTACHMENT B
Items to be Seized

I. Section I - Information to be disclosed by Google, for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of **Google**, regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to **Google**, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), including on about August 10, 2020 (**Google Reference #3924850**), **Google** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- (a) The contents of all emails associated with the account from **January 1, 2019 to the present**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- (b) All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date), account status, and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) language settings;
- (c) Google Search Console content and search history associated with the account from **January 1, 2019 to the present**;
- (d) Google Web & Activity content and web browsing history associated with the account from **January 1, 2019 to the present**;
- (e) Google Location History content and other location data, including GPS, Wi-Fi, or cell tower proximity records, from **January 1, 2019 to the present**;
- (f) Contact lists, buddy lists, and address books;

- (g) Google Voice content, including any stored voicemails and messages;
- (h) Google Chrome Sync content;
- (i) Google Chat/Messenger information and/or records, including any contact or friend list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on servers;
- (j) Google Drive content (including backups of any apps stored on Google Drive;
- (k) Google Calendar content;
- (l) Google Maps content;
- (m) Google Photos content;
- (n) Google Hangouts content;
- (o) Google Developer Console content;
- (p) Google Docs content;
- (q) Google Domains records, including records related to any registered or hosted domains;
- (r) All privacy and account settings;
- (s) Records of all changes to the account information and account settings;
- (t) All logs records of account activity related to the account;
- (u) All information about connections between the account and third-party websites and applications;
- (v) All records pertaining to communications between your entity and the account holder (or a representative thereof) regarding the account, including contacts with support services, and all records of actions taken, including suspensions of the account;
- (w) All complaints and records relating to any adverse action taken on the account, including an account suspension for violations of terms of service, whether temporary or permanent, the details surrounding that adverse action, and any communications related thereto;
- (x) List of linked accounts (collectively the “Linked Subject Accounts”) based on the following:

- i. a list of all other accounts linked by cookie overlap with any TARGET ACCOUNT;
 - ii. a list of all other accounts that list the same SMS phone number as the TARGET ACCOUNT;
 - iii. a list of all other accounts that list the same recovery email address as the TARGET ACCOUNT; and,
 - iv. a list of all other accounts that shared the same creation IP address as the TARGET ACCOUNT within 30 days of creation.
- (y) Subscriber records for each of the Linked Subject Accounts (non-content), including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) language settings.

Provider is hereby ordered to disclose the above information to the government within 14 DAYS of receipt of service of this warrant.

II. Section II - Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 1343 (Wire Fraud), Section 1030 (Computer Fraud and Abuse), Section 1029 (Access Device Fraud), and 371 and 1349 (Conspiracy to Commit such Offenses), those violations occurring between at least November 2019 to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence of any attempt or plan to engage in computer hacking or unauthorized access to networks, servers, accounts, or repositories;

- (b) Evidence of any attempt or plan to leak, publish, or otherwise disseminate source code or other data and information belonging to a third party;
- (c) Evidence of any attempt or plan to solicit or otherwise obtain source code or other data and information belonging to a third party;
- (d) Evidence of any attempt or plan to promote or solicit computer hacking or unauthorized access to networks, servers, accounts, or repositories;
- (e) Any reference to git, git.rip, exconfidential, or other accounts utilizing or incorporating the moniker “deletescape”;
- (f) Evidence of the identity of the user(s) of the account;
- (g) Evidence of the location or whereabouts, both current and historical, of the user(s) of the account;
- (h) Evidence indicating the account user’s state of mind as it relates to the crime under investigation;
- (i) Evidence of the identity or location of co-conspirators engaged in criminal conduct;
- (j) All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;
- (k) Any address lists or buddy/contact lists associated with the specified account, and other information regarding potential co-conspirators, criminal associates, or suspected victims or targets (i.e., attempted victims) of the hacking conduct and scheme;
- (l) Evidence of ownership or use of any items used to facilitate the fraudulent scheme or the existence and location of any proceeds;
- (m) All subscriber records, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;
- (n) Any and all other log records, including IP address captures;

- 1 (o) Any records of communications between Provider, and any person about
2 issues relating to the account, such as technical problems, billing inquiries,
3 or complaints from other users about the specified account. This to include
4 records of contacts between the subscriber and the provider's support
5 services, as well as records of any actions taken by the provider or
6 subscriber as a result of the communications;
7
8 (p) Any complaints and records relating to any adverse action taken on the
9 account, including an account suspension for violations of terms of service,
10 whether temporary or permanent, the details surrounding that adverse
11 action, and any communications related thereto.
12
13

14 This warrant authorizes a review of electronically stored information, communications,
15 other records and information disclosed pursuant to this warrant in order to locate
16 evidence, fruits, and instrumentalities described in this warrant. The review of this
17 electronic data may be conducted by any government personnel assisting in the
18 investigation, who may include, in addition to law enforcement officers and agents,
19 attorneys for the government, attorney support staff, and technical experts. Pursuant to
20 this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the
21 custody and control of attorneys for the government and their support staff for their
22 independent review.
23
24
25
26
27
28

CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Google LLC** (“Provider”), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Provider. The attached records consist of

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Provider, and they were made by Provider as a regular practice; and

b. such records were generated by Provider’s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Provider in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Provider, and at all times pertinent to the records certified here the process and system functioned properly and normally.

1 I further state that this certification is intended to satisfy Rules 902(11) and
2 902(13) of the Federal Rules of Evidence.

3
4
5 Date

Signature